KONGERIKET NORGE
The Kingdom of Norway

Bekreftelse på patentsøknad nr
Certification of patent application no

1999 4334

Det bekreftes herved at vedheftede dokument er nøyaktig utskrift/kopi av ovennevnte søknad, som opprinnelig inngitt 1999.09.06

It is hereby certified that the annexed document is a true copy of the above-mentioned application, as originally filed on 1999.09.06

2000.07.27

Freddy Strømmen

Freddy Strømmen
Seksjonsleder

Eli Edvardsen

Eli Edvardsen

PATENTSTYRET
Styret for det industrielle rettsvern

BL. - 130 - 5000 - 8.98 - Lørenskog Trykk as

PATENTSTYRET
Styret for det industrielle rettsvern

ADRESSE
Postboks 8160 Dep.
Københavngaten 10
0033 Oslo

TELEFON
22 38 73 00
TELEFAKS
22 38 73 01

BANKGIRO
8276.01.00192
FORETAKSNUMMER
971526157

1999 -09- 06 Ingen avgift

PATENTSTYRET

06.SEP99 994334

Søknad om patent

Søknadsskriv

1a - e

Utfylles av styret
Behandlende medlem EK
Int. Cl.[6] H04L

Søkers/fullmektigens referanse (angis hvis ønsket):
O. nr. E09816
JFW/OG

Alm. tilgj. 07 MARS 2001

Oppfinnelsens benevnelse:

Sikkerhet med autentiseringsproxy.

Hvis søknaden er en internasjonal søknad som videreføres etter patentlovens § 31:

Den internasjonale søknads nummer .....

Den internasjonale søknads inngivelsesdag .....

Søker:
Navn, bopel og adresse.
(Hvis patent søkes av flere: opplysning om hvem som skal være bemyndighet til å motta meddelelser fra Styret på vegne av søkerne).

(Fortsett om nødvendig på neste side)

TELEFONAKTIEBOLAGET LM ERICSSON
SE-126 25 Stockholm
Sverige

Oppfinner:
Navn og (privat-) adresse

(Fortsett om nødvendig på neste side)

se eget ark

Fullmektig:

BRYNS PATENTKONTOR A/S
Karl Johansgt. 25
P.O.Box 765 Sentrum
N-0106 Oslo

Hvis søknad tidligere er inngitt i eller utenfor riket:

(Fortsett om nødvendig på neste side)

Prioritet kreves fra dato ..... sted ..... nr. .....

Prioritet kreves fra dato ..... sted ..... nr. .....

Prioritet kreves fra dato ..... sted ..... nr. .....

Hvis avdelt søknad:

Den opprinnelige søknads nr.: ..... og deres inngivelsesdag .....

Hvis utskilt søknad:

Den opprinnelige søknads nr.: ..... begjært inngivelsesdag .....

Deponert kultur av mikroorganisme:

☐ Søknaden omfatter kultur av mikroorganisme

Utlevering av prøve av kulturen:

☐ Prøve av den deponerte kultur av mikroorganisme skal bare utleveres til en særlig sakkyndig, jfr. patentlovens § 22 åttende ledd og patentforskriftenes § 38 første ledd

994334

Angivelse av tegnings-figur som ønskes publisert sammen med sammendraget

Fig. nr. .....

BL. 10 10.000 - 05.99 Lørenskog Trykk

Security with authentication proxy

Field of invention.

The present invention relates to the field of audio, video and data communications across packet based networks, particularly to authentication of end-users and end-points in networks complying with the H.323 specification of the International Telecommunications Union.

The problem areas.

The ITU-T recommendation H.235 of the International Telecommunications Union recommends a standard for security and encryption for multimedia terminals complying with the H-Series recommendations (H.323 and other H.235-based) of International Telecommunications Union. H.235 is a new feature in version 2 (H.323v2) of the H.323 recommendation. It adds various security mechanisms like authentication and integrity checks to the recommended standard H.323. In version 1 (H.323v1) of the H.323 there were no security mechanisms, and the network had to trust that the end-users were who they claimed to be. This constitutes a problem when end-users have their own confidential profiles in the system including a set of supplementary services. End-user authentication is a pre-requisite when billing the end-user for the H.323 traffic, and when building virtual private networks on the H.323 network.

Even though the use of H.235 looks promising, some major problems remain to be solved. One problem is that there is a wide use of H.323 version 1 end-points in use. As stated above, only end-points complying with H.323v2 can support H.235. Another problem is that very few of the end-points complying with H.323v2 that are on the marked today support H.235. Both of these problems need to be solved in an H.323 network which base its logic on authenticated end-users.

Another problem area is H.235 itself, since it is very generic and needs a security profile to be applied. In a network it is likely that many different security profiles will be in use by different end-points. When security profiles are different, conversion of one security profile to another security profile cannot be made since the security profiles generally will perform different hash function on different data. As a consequence it is not practical for the H.323 network components to support all security profiles.

An example to illustrate the problem with two clients with different security profiles is shown in fig 1. In this example the gatekeeper (3) needs to support both security profiles to be able to authenticate both end-users (1) using the two H.323 clients.

Known Solutions and problems with these.

One solution to the problems with H.235 is to not base the authentication on H.235 at all, and use a proprietary protocol for end-user (1) authentication. This in turn leads to two problems:

1) The end-user (1) has to start two programs, the authentication client, and the H.323 client when using the H.323 network even though the H.323 client is a version 2 client with H.235 support.

2) The H.323 network has to support a new proprietary protocol in addition to H.323.

Another known solution is to apply the IMTC Security Profile 1 (SP1) proposed by the International Multimedia Teleconferencing Consortium. It is however focused on message by message authentication and integrity, and has not made a clear distinction between user authentication and message integrity.

Objects of the invention

Accordingly, it is an object of the present invention to provide an arrangement in a H.323 network which will allow authentication of end-points that comply with H.323v1.

Another object of the present invention is to provide an arrangement in a H.323 network which will allow authentication of end-points that comply with H.323v2 but do not support H.235.

A further object of the present invention is to provide an arrangement in a H.323 network which will allow authentication of end-users (1) clients with different security profiles.

Brief description of the invention

The above objects are met in an arrangement provided by the present invention, wherein an authentication proxy is provided and a gatekeeper supports a security profile used by an authentication proxy .

Description of the drawings:

fig. 1 shows an example of a prior art arrangement in which the gatekeeper (3) encounters different clients with different security profiles,

fig. 2 shows an example of an arrangement according to the invention,

fig. 3 shows an example of signal flow of an arrangement according to the invention.

Detailed description of embodiments.

In the following, by way of example the present invention will be described in more detail.

Referring to fig. 2, an example of an embodiment of the present invention is shown. All information the authentication proxy (2) needs, will be requested from the end-user (1) through standard http communication or any other suitable protocol.

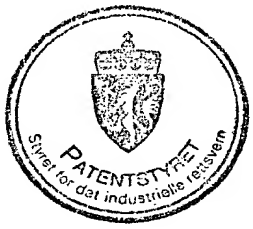
In the following, only for the purpose of explaining the present invention the protocol used will be http.

An end-user (1) could be presented a simple html form, an applet (that can be signed), a servlet or likewise for providing his/her user name and password.

The hashing described in the H.235 security profile should be done by the applet if an applet is used. If the hashing is not performed by the applet, or something else than an applet is used, the communication protocol should instead be SSL, i.e. https instead of http. Then the hashing will be performed in the authentication proxy (2). In this way the information will be secure all the way.

Referring to fig. 3, signal flow is explained in the following by way of example. When the authentication proxy (2) receives the information from the user, it generates a standard RAS message such as a H.323v2 GRQ (gatekeeper Request), which holds the H.235 data. This is sent directly to a gatekeeper (3) according to H.323v2, where the actual authentication is done. The H.323 client can register with the gatekeeper (3) in a normal way. The gatekeeper (3) will know that the user/end-point (1) already is authenticated based on the user name, the Internet Protocol(IP)-address or both.

To avoid problems in the gatekeeper (3) when receiving two GRQ's (one from the proxy (2) and one from the end-point (1)), the authentication proxy (2) can answer GRQ's sent from end-points (1) complying with H.323v1 and end-points (1) complying with H.323v2 without H.235 support directly. Because the gatekeeper (3) will only receive H.323v2 GRQ's when this feature is added, the gatekeeper (3) can not, based on the GRQ, decide which version of the H.323 the various end-points (1) are complying with. The Gatekeeper (3) should instead base it decision on the received RRQs or other suitable RAS messages from endpoints.



Patent claims.

1.
An arrangement for audio, video, and data communications across packet based networks implementing the H.323 standard recommended by the International Telecommunications Union, the arrangement including one ore more gatekeepers (3), characterised in
that end-user (1) authentication is performed by means of an authentication proxy (2).

2.
An arrangement according to claim 1, characterised in
that a security profile used by an authentication proxy (2) is supported by a gatekeeper (3) associated with said authentication proxy (2).

3.
An arrangement according to claim 1 or 2, characterised in
that end-user information needed by an authentication proxy (2) is requested from the end-user (1) by means of a non-proprietary communications protocol.

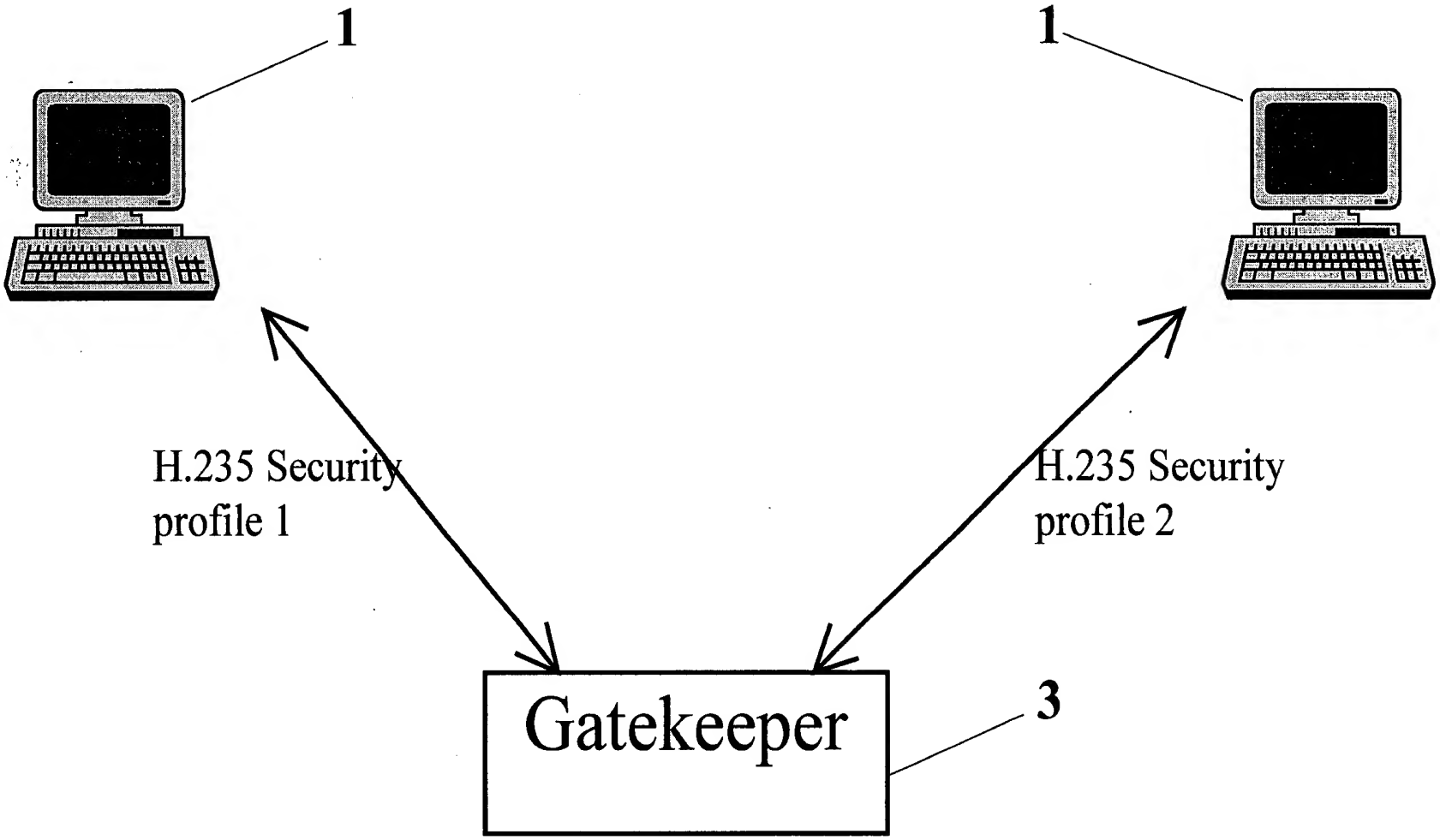
4.
An arrangement according to claim 1, 2 or 3, characterised in
that an authentication proxy (2) communicates information to a gatekeeper (2) by means of a H.323 version 2 RAS message.

5.
An arrangement according to claim 3, characterised in
that a non-proprietary communications protocol is selected form a group of non-proprietary protocols comprising http and https.

6.
An arrangement according to claim 1 or 2, characterised in
that information for end-user (1) authentication is provided by the end-user (1) by means of a html form, an applet or a servlet.

Abstract.

An arrangement to accomplish authentication of end-users (1) and end-points (1) in a packet based network which includes components that support all or parts of different versions of the H.323 recommended standard is proposed. Authentication is accomplished by means of an authentication proxy (2) which will support security profiles supported by one or more associated gatekeepers (3). Provision of end-user (1) and end-point information for an authentication proxy (2) may be accomplished by means of standard non-proprietary communication and protocol such as http or https and a simple html form, an applet or a servlet respectively, and for a gatekeeper (3) by means of a RAS message such as gatekeeper request (GRQ).



PRIOR ART

Fig. 1

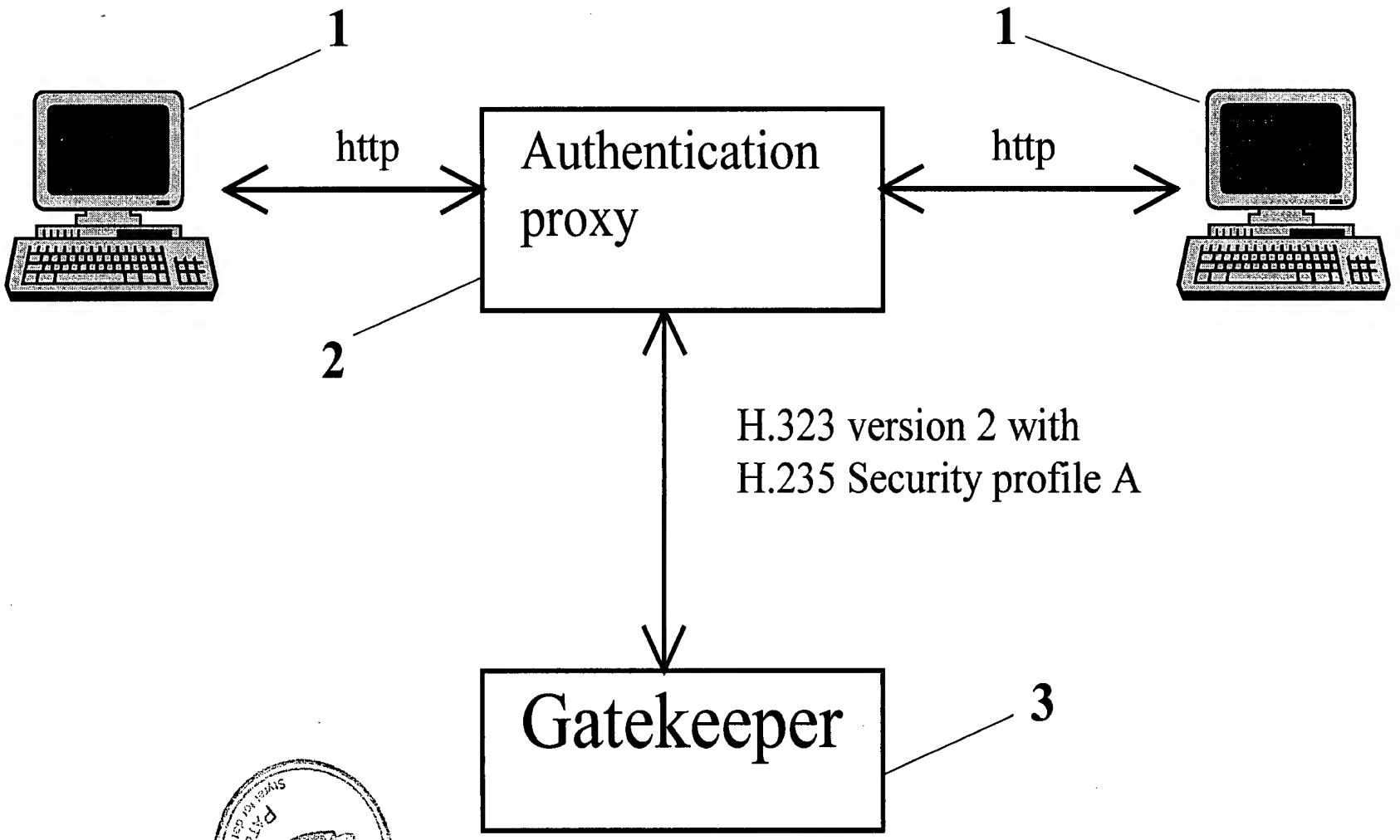

1
1
http
http
Authentication
proxy
2
H.323 version 2 with
H.235 Security profile A
Gatekeeper
3

Fig. 2

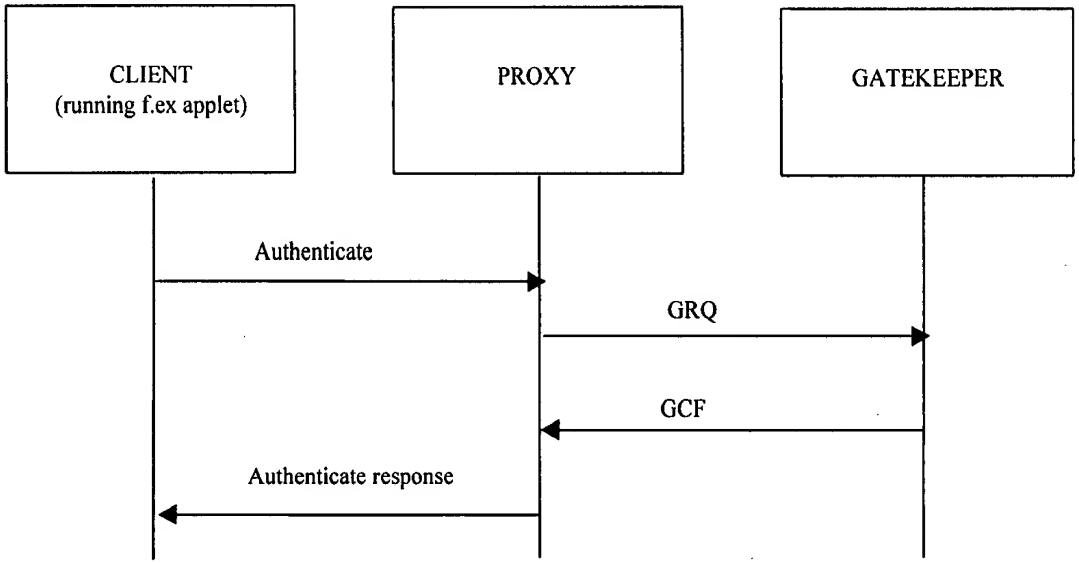


Fig. 3